

Valence bond solid formalism for d-level one-way quantum computation*

Sean Clark[†]

February 1, 2008

Abstract

The d-level or qudit one-way quantum computer (d1WQC) is described using the valence bond solid formalism and the generalised Pauli group. This formalism provides a transparent means of deriving measurement patterns for the implementation of quantum gates in the computational model. We introduce a new universal set of qudit gates and use it to give a constructive proof of the universality of d1WQC. We characterise the set of gates that can be performed in one parallel time step in this model.

1 Introduction

Since its introduction the one-way quantum computer (1WQC) [1, 2] has sparked interest in areas including the study of resources for quantum computation, the complexity of algorithms [3], and practical implementation schemes for quantum computing [4, 5, 6, 7, 8].

Comparing the 1WQC with the standard quantum circuit (QC) model allows us to ask questions about the resources required for quantum computation. The standard QC model requires (at least in a perfect world) preparation of the zero state, controlled unitary evolution of a universal set of gates and measurement in the computational basis. This compares to the 1WQC which requires preparation of a multipartite entangled cluster state and the ability to perform measurements in classically computed adaptive bases. There have also been comparisons [9, 10, 11, 12, 13] showing that the 1WQC is equivalent to another model of measurement based quantum computation known as teleportation-based quantum computation (TQC) [14, 15]. The valence bond solid (VBS) formalism [12] of the 1WQC provides a fundamental basis for such a comparison.

Here we extend the use of the VBS formalism to describe the workings of the 1WQC for d-level systems or qudits which is known as the d-level one-way quantum computer (d1WQC). The d1WQC was first introduced in [16] in which its workings are described in terms of an irreducible representation of Manin's quantum plane algebra [17]. The VBS formalism

*A preliminary version of this work was presented in a poster at the CNRS summer school on Quantum Logic and Communication, Corsica August 2004.

[†]Department of Computer Science, University of Bristol, Woodland Road, Bristol, BS8 1UB, England.
email: sean.clark@bristol.ac.uk

provides a clear representation of the workings of the d1WQC and opens the way for a variety of natural generalisations.

The construction of the d1WQC given here exposes a special role of the group of generalised Clifford operations: quantum circuits of such operations, when implemented on the d1WQC can be performed in one parallel measurement time step followed by poly-logarithmic classical processing. We give a full characterisation of the Clifford group of circuits for d-level systems in the appendix that differs from the more formal approach of [18].

The workings of the qubit 1WQC were introduced in [1, 2] and a review of this and measurement-based quantum computation is given in [13]. Computation in this model proceeds by producing a highly entangled state called a cluster state and then performing measurements on each of the qubits. The cluster state is described by the local interactions between its constituent quantum systems. Each qubit in the cluster is measured during the computation using one-qubit projective measurements in a chosen basis that may be calculated classically from any previous measurement results. The specification of the cluster state and choice of basis for each of the measurements together define the algorithm performed. The d1WQC is a natural extension of the 1WQC in which the constituent systems are d-level quantum systems or qudits. We describe an arbitrary d-level cluster state constructed from the VBS picture using the generalised Pauli group of quantum gates which are defined in the next section. We also show how to perform a universal set of gates on multi-qudit systems in this model.

The paper proceeds as follows. We start by defining the Pauli and Clifford groups for qubits and their generalisations to systems of qudits and prove a theorem characterising the Clifford group in prime dimension. We proceed to give definitions of cluster states and a VBS states of qudits and show that a cluster state can be obtained from a VBS state by applying a suitable projector. We then go on to describe the workings of teleportation-based quantum computation on VBS states by constructing a parameterised one-qudit gate and the two-qudit generalised controlled-Z gate. We show how these constructions can be concatenated and prove that they allow for universal quantum computation. Next we show how the same projector can be used to transparently derive measurement schemes for gate implementations on the d1WQC. Finally we mention the implications of this formalism for the parallel complexity of generalised Clifford circuits.

2 The generalised Pauli group

A basic ingredient in our description of the workings of the d1WQC is the generalised Pauli group of quantum gates. In this section we review the Pauli group for systems of qubits and describe the natural extension to systems of qudits. We also define the Clifford group of gates that normalise the Pauli group. In doing so we establish the notation used throughout the paper.

The Pauli group of quantum gates on one qubit, denoted \mathcal{P}_2 , is defined in terms of its generators σ_x and σ_z . $\mathcal{P}_2 = \langle \sigma_x, \sigma_z \rangle$ where $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, and $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

We note that this differs from the usual definition which usually includes the gate $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ amongst the generators. We will refer to our definition as the real Pauli group and the more usual definition as the complex Pauli group.

We extend the Pauli group by tensor products, leading to the Pauli group on n -qubits, $\mathcal{P}_2^{\otimes n}$, such that

$$\mathcal{P}_2^{\otimes n} = \left\{ \bigotimes_{k=1}^n p_k : p_k \in \mathcal{P}_2 \right\}. \quad (2.1)$$

The normaliser $\mathcal{N}_U(G)$ of any complex matrix group $G \subset U(d)$ within the unitary group $U(d)$ is defined to be

$$\mathcal{N}_{U(d)}(G) = \left\{ N \in U(d) : \forall A \in G, \exists A' \in G, c \in \mathbb{C} \text{ s.t. } N A N^\dagger = c A' \right\}. \quad (2.2)$$

Note that this differs from the standard mathematical definition in that we allow for an extra constant c (which necessarily has unit modulus).

The Clifford group on n qubits is defined as being the normaliser of the Pauli group within the unitary group.

$$\mathcal{Cl}_2^{\otimes n} = \mathcal{N}_{U(2^n)}(\mathcal{P}_2^{\otimes n}). \quad (2.3)$$

The more general definition of normaliser is justified in the current context since both in teleportation and quantum computation we consider two elements of the Pauli group to be equivalent if they differ only by some global phase factor. We also note that in using our definition the real and complex Pauli groups have the same normaliser whereas they do not given the standard definition.

Some further gates used in this paper are the following. The one-qubit Hadamard gate is

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (2.4)$$

The $\frac{\pi}{4}$ phase gate is

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}. \quad (2.5)$$

The two-qubit controlled-NOT gate is

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \quad (2.6)$$

The controlled-Z gate is

$$C_Z = \text{diag}(1, 1, 1, -1) \quad (2.7)$$

where diag denotes a diagonal matrix with the given entries.

In fact H , S , $CNOT$ and C_Z are all gates in the Clifford group and furthermore it was shown in [19] that, up to a global phase factor, H and S together generate \mathcal{Cl}_2 and H , S , and $CNOT$ together generate $\mathcal{Cl}_2^{\otimes n}$ for any n .

We now define the natural generalisation of the Pauli group to systems of qudits.

Let the one qudit gates X and Z be such that for $j \in \mathbb{Z}_d$ (where \mathbb{Z}_d denotes the ring of integers modulo d sometimes denoted $\mathbb{Z}/d\mathbb{Z}$)

$$X|j\rangle = |j+1(\text{mod } d)\rangle \quad (2.8)$$

$$Z|j\rangle = \omega^j|j\rangle \quad (2.9)$$

where $\omega = \exp\left(\frac{2\pi i}{d}\right)$ is the d^{th} root of unity. We note the fundamental relation

$$ZX = \omega XZ. \quad (2.10)$$

Definition 2.1. The generalised Pauli group on one qudit, $\mathcal{P}_d = \langle X, Z \rangle$, is defined to be the group generated by X and Z , and the Pauli group on n qudits is defined as

$$\mathcal{P}_d^{\otimes n} = \left\{ \bigotimes_{k=1}^n p_k : p_k \in \mathcal{P}_d \right\}. \quad (2.11)$$

Using the relation $ZX = \omega XZ$ we note that we can express $\mathcal{P}_d^{\otimes n}$ as

$$\mathcal{P}_d^{\otimes n} = \left\{ \omega^k Z_1^{a_1} X_1^{b_1} \dots Z_n^{a_n} X_n^{b_n} : a_j, b_j, k \in \mathbb{Z}_d \right\} \quad (2.12)$$

Here the subscripts label upon which qudit the operator acts. Often we will not be interested in the the global phase ω^k . In this case we may considered the central quotient group $\mathcal{P}_d^{\otimes n} / Z(\mathcal{P}_d^{\otimes n})$ (where $Z(\mathcal{P}_d^{\otimes n})$ denotes the centre of the group) with representatives of the form $Z_1^{a_1} X_1^{b_1} \dots Z_n^{a_n} X_n^{b_n}$.

Definition 2.2. The Clifford group on n qudits, $\mathcal{Cl}_d^{\otimes n}$, is defined to be the normaliser of $\mathcal{P}_d^{\otimes n}$ in $U(d^n)$. That is

$$\mathcal{Cl}_d^{\otimes n} = \mathcal{N}_{U(d^n)}(\mathcal{P}_d^{\otimes n}). \quad (2.13)$$

The generalisation to the qudit case of the H , S , controlled-NOT and controlled-Z gates are as follows. H becomes the quantum Fourier transform on one qudit, which we denote by F .

$$F|j\rangle = \frac{1}{\sqrt{d}} \sum_{m \in \mathbb{Z}_d} \omega^{jm} |m\rangle \quad (2.14)$$

For the case where d is odd we have the definition

$$S|j\rangle = \omega^{\frac{j}{2}(j+1)} |j\rangle \quad (2.15)$$

and

$$C_X|j\rangle|k\rangle = |j\rangle|j+k(\text{mod } d)\rangle, \quad C_Z|j\rangle|k\rangle = \omega^{jk}|j\rangle|k\rangle. \quad (2.16)$$

In the appendix we give a proof of the following theorem:

Theorem 2.3. Any Clifford circuit on n qudits, where d is an odd prime, can be constructed as quantum circuit up to a global phase from the gates $\{C_X, F, S\}$.

3 Cluster states of qudits in the VBS formalism

Central to the workings of the one-way quantum computer (1WQC) is the cluster state [20]. Here we give a constructive definition of cluster states of qudits.

Definition 3.1. A cluster state consists of a lattice of qudits with some given neighbourhood scheme. Each of the qudits on the lattice is individually prepared in the $|+\rangle$ state where

$$|+\rangle = \frac{1}{\sqrt{d}} \sum_{j \in \mathbb{Z}_d} |j\rangle. \quad (3.1)$$

Then the two-qudit controlled-Z gate, C_Z (as defined in equation 2.16), is applied once between each neighbouring pair of qudits.

In this paper we will consider only linear and square lattices as they are sufficient for universal quantum computation.

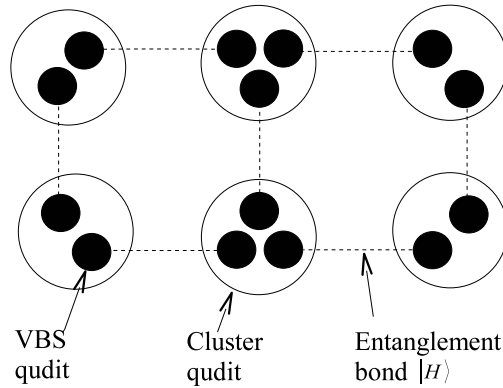


Figure 1: An example VBS state

In the VBS formalism we describe the cluster state using a VBS state (generalising the procedure given for $d = 2$ in [12]). A VBS state consists of pairs of qudits entangled in the state $|H\rangle$ as in figure 1.

$$|H\rangle = C_Z |+\rangle |+\rangle = \sum_{j,k \in \mathbb{Z}_d} \omega^{jk} |j\rangle |k\rangle. \quad (3.2)$$

Here we have ignored and shall continue to ignore normalisation factors throughout this paper. Further properties of VBS states can be found in [21, 22].

Given a particular cluster state we consider a corresponding VBS state with one pair of qudits entangled in the $|H\rangle$ state for each neighbouring pair of cluster qudits as shown in figure 1.

We now show that the cluster state “resides inside” the corresponding VBS state, within the d -dimensional subspaces spanned by $|j\rangle \dots |j\rangle$ for $j \in \mathbb{Z}_d$ at each site of the VBS state.

Theorem 3.2. *For any VBS state introduce the projector*

$$\Pi_a = \sum_{j \in \mathbb{Z}_d} |\tilde{j}\rangle \langle j| \dots \langle j| \quad (3.3)$$

at each site a where we have used a tilde to re-label the basis states after projection. If we apply Π_a for all a to the VBS state we obtain (after re-normalising) the corresponding cluster state.

To prove the theorem we show that the combined action of the projector Π_a at each site does indeed produce a cluster state on lattices of one and two dimensions. Starting with the one-dimensional case we consider the lattice in figure 2

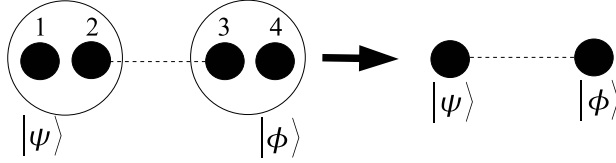


Figure 2: Projecting one VBS bond to a cluster state

Ignoring normalisation factors, the state on the left hand side of figure 2 is

$$|\psi\rangle_1 |H\rangle_{23} |\phi\rangle_4 = \sum_j \psi_j |j\rangle_1 \sum_{mn} \omega^{mn} |m\rangle_2 |n\rangle_3 \sum_k \phi_k |k\rangle_4. \quad (3.4)$$

The projector to apply is

$$\sum_p |\tilde{p}\rangle \langle p|_1 \langle p|_2 \otimes \sum_q |\tilde{q}\rangle \langle q|_3 \langle q|_4. \quad (3.5)$$

This gives the state

$$\sum_{jkmnpq} \psi_j \phi_k \omega^{mn} \langle p|j\rangle \langle q|m\rangle \langle q|n\rangle \langle q|k\rangle |\tilde{p}\rangle |\tilde{q}\rangle = \sum_{pq} \psi_p \phi_q \omega^{pq} |\tilde{p}\rangle |\tilde{q}\rangle \quad (3.6)$$

$$= C_Z |\tilde{\psi}\rangle |\tilde{\phi}\rangle. \quad (3.7)$$

Using the derivation in equation 3.7 we can extend this result to an arbitrary one-dimensional cluster state. In figure 3 the dashed lines already represent $C_Z|+\rangle|+\rangle$ and we see that the projectors on sites 23 and 45 have the effect of applying a further C_Z gate between the corresponding cluster sites. This is true as we continue down the lattice leaving a 1-dimensional cluster state.

In the more general case of a two-dimensional cluster state we consider a VBS state site which represents a cluster qudit with four neighbours shown in figure 4.

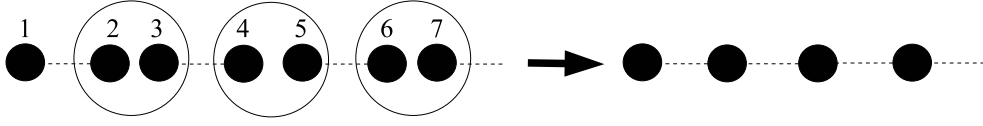


Figure 3: Projecting to a cluster state on a one-dimensional lattice

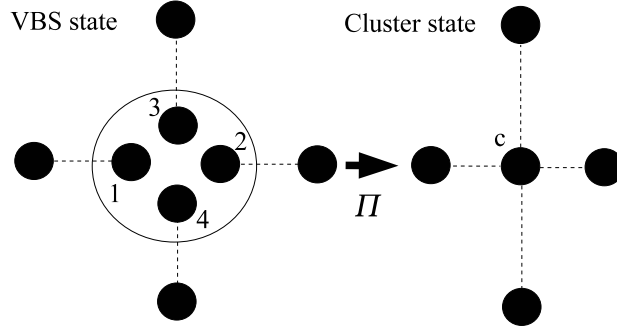


Figure 4: A VBS state cluster state on a two dimensional lattice

The projector Π for this cluster qudit is given by

$$\Pi = \sum_k |\tilde{k}\rangle \langle k|_1 \langle k|_2 \langle k|_3 \langle k|_4. \quad (3.8)$$

Which we can decompose into the sequential application of Π_1 , Π_2 and Π_3 where

$$\Pi_1 = \sum_k |\tilde{k}\rangle_a \langle k|_1 \langle k|_2, \quad \Pi_2 = \sum_k |\tilde{k}\rangle_b \langle k|_a \langle k|_3, \quad \Pi_3 = \sum_k |\tilde{k}\rangle_c \langle k|_b \langle k|_4. \quad (3.9)$$

Hence the result in equation 3.7 applied successively shows that in general any two-dimensional VBS state will project down to a cluster state completing the proof of the theorem.

4 Teleportation-based quantum computation on VBS states

In this section we describe how to perform universal quantum computation on VBS states using teleportation-based quantum computation (TQC) [14, 15]. In section 5 we show that this gives the functioning of the d-level one-way quantum computer (d1WQC) [16] in the subspace that the cluster state resides in.

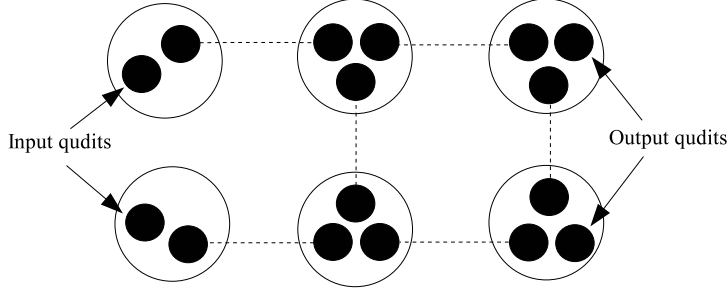


Figure 5: Input and output in the VBS picture

4.1 Input and output qudits in the VBS formalism

Qudits that do not form part of a $|H\rangle$ bond are used for input and output. The input qudits are placed as shown in figure 5 in the desired state. The output qudits are measured in the computational basis and these results are corrected using calculations from the other measurement results to form the classical output from the computation as we describe in the following.

4.2 Universality for quantum computation

We show how to implement a universal set of gates on a VBS state. The gates used are a parameterised one-qudit gate and the controlled-Z gate between two qudits. As shown in the following these gates are implemented up to a random unitary error which is in the generalised Pauli group as described in section 2. We show how these errors can be deterministically corrected for.

4.2.1 A parameterised one-qudit gate

In order to implement any one qudit gate we show that we implement any gate of a special form $U(\vec{c})$ that is parameterised by a vector $\vec{c} = (c_0 = 1, c_1, \dots, c_{d-1})$ of d complex numbers of modulus one. The gate $U(\vec{c})$ is defined as

$$U(\vec{c})|j\rangle = F \text{diag}(\vec{c}) = c_j \sum_{m \in \mathbb{Z}_d} \omega^{jm} |m\rangle. \quad (4.1)$$

This particular set of gates is chosen because as shown in section 5.1 they have special properties in relation to the projectors Π_a . $U(\vec{c})$ is implemented on a VBS state as a d -dimensional analog of the TQC as shown in figure 6. Qudits 1 and 2 are measured in the basis B defined as

$$B = \{|\alpha_{st}\rangle = (U(\vec{c})^\dagger X^s Z^t \otimes I)|H\rangle : s, t \in \mathbb{Z}_d\}. \quad (4.2)$$

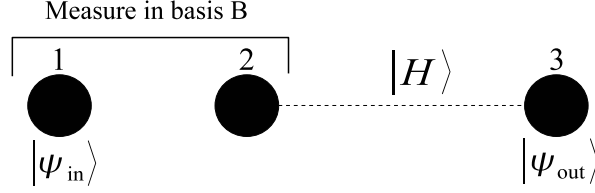


Figure 6: Implementing the $U(\vec{c})$ gate modulo a random Pauli error

We can see that the basis B is a ‘twisted’ generalised Bell basis and that so is equivalent to preparing qudit 1 in the state $U(\vec{c})|\psi\rangle$ and measuring in the (untwisted) generalised Bell basis. If the measurement result is $s, t \in \mathbb{Z}_d$ then we have teleported [23, 24] the state $U(\vec{c})|\psi\rangle$ and qudit 3 is left in the state

$$Z^{-t}X^{-s}U(\vec{c})|\psi\rangle. \quad (4.3)$$

Next we will show that the known Pauli error $Z^{-t}X^{-s}$ which is produced by the act of teleportation can be corrected for.

4.2.2 Combining multiple $U(\vec{c})$ gates

We have shown how to implement the gate $U(\vec{c})$ modulo some random Pauli error Z^tX^s . Since s and t are known these errors can be tracked and corrected for. In order to do this when combining multiple $U(\vec{c})$ gates we will propagate all the errors to the end of the computation and correct for them last. For this we need the commutation relations of $U(\vec{c})$ with all Pauli errors. It suffices to calculate them for the generators X, Z of the Pauli group.

We introduce the following notation. If $\vec{c} = (c_0, c_1, \dots, c_{d-1})$ then $\vec{c}_{++} = (c_1, c_2, \dots, c_{d-1}, c_0)$. This gives

$$U(\vec{c}_{++})|j\rangle = c_{j+1} \sum_{m \in \mathbb{Z}_d} \omega^{jm} |m\rangle. \quad (4.4)$$

Calculating the propagation for Z and $U(\vec{c})$ we have

$$U(\vec{c})Z|j\rangle = U(\vec{c})\omega^j|j\rangle = c_j \sum_{m \in \mathbb{Z}_d} \omega^{j(m+1)} |m\rangle = X^{-1}U(\vec{c})|j\rangle \quad (4.5)$$

Similarly for X and $U(\vec{c})$ we have

$$U(\vec{c})X|j\rangle = U(\vec{c})|j+1\rangle = c_{j+1} \sum_m \omega^{m(j+1)} |m\rangle = ZU(\vec{c}_{++})|j\rangle \quad (4.6)$$

Hence we have the propagation relations

$$U(\vec{c})Z = X^{-1}U(\vec{c}) \quad (4.7)$$

and

$$U(\vec{c})X = ZU(\vec{c}_{++}) \quad (4.8)$$

These relations allow us to implement many such gates of the form $U(\vec{c})$ and avoid having to correct the errors after each one by adapting the implementation of each gate depending upon the errors produced up to that point and tracking the errors for a future gate implementation. This adds a requirement of performing steps of classical computation in between the measurement steps into the computational model.

At the end of the computation we restrict the output measurements to be in the computational basis. Since each output qudit carries a Pauli error of $Z^t X^s$ if we obtain the measurement result $m \in \mathbb{Z}_d$ we correct by taking the final result to be $m - s(\text{mod } d)$ since the Z errors have no effect to measurements in the computational basis.

4.2.3 Implementing C_Z

We implement the controlled- Z gate, C_Z , on the VBS state as in figure 7. We use a three-qudit measurement in a basis B_2 where

$$B_2 = \left\{ X^r \otimes Z^s \otimes X^t \left(\sum_{m \in \mathbb{Z}_d} |m\rangle |m\rangle |m\rangle \right) : r, s, t \in \mathbb{Z}_d \right\} \quad (4.9)$$

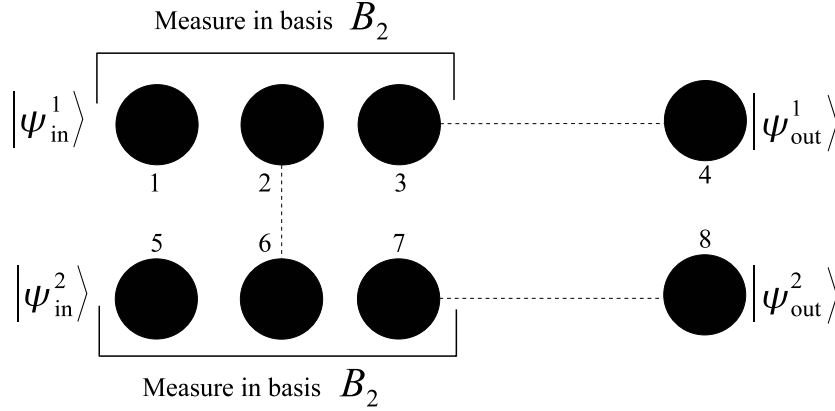


Figure 7: Implementing a generalised C_Z gate

We denote a C_Z gate applied between qudits j and k by $C_{Z(j,k)}$ where qudits j and k are the control and target qudits respectively. The following lemma applies to figure 7.

Lemma 4.1. *After measurement of qudits 1,2,3 in basis B_2 with measurement results $r, s, t \in \mathbb{Z}_d$ and measurement of qudits 5,6,7 in basis B_2 with results $u, v, w \in \mathbb{Z}_d$ the state of the subsystem consisting of qudits 4 and 8 is, up to a global phase, equal to*

$$Z_4^{t-r} Z_8^{w-u} X_4^{s+u} X_8^{v+r} F_4 F_8 C_{Z(4,8)} |\psi_{in}^1\rangle_4 |\psi_{in}^2\rangle_8. \quad (4.10)$$

This proof of this lemma is given in appendix B.

The implementation of C_Z , up to Pauli errors, is completed by applying the inverse Fourier transform, F^\dagger , to both output qudits using the techniques described in the previous section and theorem 4.2 below.

4.2.4 Combining other gates with C_Z

We have already seen the commutation relations of the one-qudit gate $U(\vec{c})$ with the Pauli errors and how this allows us to correct for all the errors at the end of the computation. In the case of C_Z it is in the normaliser of the Pauli group with propagation relations

$$C_{Z(1,2)}Z_1 = Z_1C_{Z(1,2)}, C_{Z(1,2)}Z_2 = Z_2C_{Z(1,2)} \quad (4.11)$$

and

$$C_{Z(1,2)}X_1 = X_1Z_2C_{Z(1,2)}, C_{Z(1,2)}X_2 = Z_1X_2C_{Z(1,2)}. \quad (4.12)$$

From these relations we see that the implementation of the C_Z gate is not effected by Pauli error propagation.

4.2.5 Proof of universality

We now show that the ability to perform any gate of the form $U(\vec{c})$ and C_Z allows for universal quantum computation. Starting with the one-qudit case we have

Theorem 4.2. *Gates of the form $U(\vec{c})$ can be used to produce any one-qudit gate when d is an odd prime*

Proof. Given a linearly independent set $\{H_j\}$ of d^2 hermitian matrices (each of size $(d \times d)$) we can write any unitary $U \in U(d)$ as

$$U = \exp(iH) = \exp\left(i \sum_{j=1}^{d^2} \alpha_j H_j\right) = \prod_{j=1}^{d^2} \exp(i\beta_j H_j) \quad (4.13)$$

for some real parameters α_j, β_j .

We now give such a set of linearly independent one-qudit Hermitian matrices and show how the corresponding one-parameter unitary gates can be implemented from gates of the form $U(\vec{c})$.

Let us choose $d + 1$ Pauli elements from \mathcal{P}_d such that the eigenvectors of these elements form a set of mutually unbiased bases [25]. Let us denote these bases as

$$\{|a_1\rangle, \dots, |a_d\rangle\}, \{|b_1\rangle, \dots, |b_d\rangle\}, \dots, \{|e_1\rangle, \dots, |e_d\rangle\}. \quad (4.14)$$

We use these vectors to form a set of d^2 Hermitian operators

$$\{|a_1\rangle\langle a_1|, \dots, |a_d\rangle\langle a_d|, |b_1\rangle\langle b_1|, \dots, |b_d\rangle\langle b_d|, |e_1\rangle\langle e_1|, \dots, |e_d\rangle\langle e_d|\} \quad (4.15)$$

where we have omitted the first vector in all bases except the first basis. We claim that this set is linearly independent. Since for any set of real numbers $\{\alpha_j, \beta_k, \epsilon_k\}_{j \in \{1, \dots, d\}, k \in \{2, \dots, d\}}$ if we have

$$\alpha_1|a_1\rangle\langle a_1| + \dots + \alpha_d|a_d\rangle\langle a_d| + \beta_2|b_2\rangle\langle b_2| + \dots + \beta_d|b_d\rangle\langle b_d| + \epsilon_2|e_2\rangle\langle e_2| + \dots + \epsilon_d|e_d\rangle\langle e_d| = 0 \quad (4.16)$$

then by applying $\langle a_j| \dots |a_j\rangle$ to each side of the equation for each value of $j \in \{1, \dots, d\}$ we obtain

$$\alpha_j + \frac{1}{\sqrt{d}}(\beta_2 + \dots + \beta_d + \epsilon_2 + \dots + \epsilon_d) = 0. \quad (4.17)$$

From this we conclude that all values of α_j are equal to α , say. Similarly we can argue that all values of β_j (\dots, ϵ_j) are equal to β (respectively \dots, ϵ). Let us now rewrite equation 4.15 as

$$\alpha(|a_1\rangle\langle a_1| + \dots |a_d\rangle\langle a_d|) + \beta(|b_2\rangle\langle b_2| + \dots |b_d\rangle\langle b_d|) + \epsilon(|e_2\rangle\langle e_2| + \dots |e_d\rangle\langle e_d|) = 0. \quad (4.18)$$

Then

$$\alpha I + \beta(I - |b_1\rangle\langle b_1|) + \dots + \epsilon(I - |e_1\rangle\langle e_1|) = 0. \quad (4.19)$$

Rearranging we have

$$(\alpha + \beta + \dots + \epsilon)I = \beta|b_1\rangle\langle b_1| + \dots + \epsilon|e_1\rangle\langle e_1|. \quad (4.20)$$

Applying $\langle b_1| \dots |b_1\rangle$ to both sides gives

$$(\alpha + \beta + \dots + \epsilon) = \beta + \frac{1}{\sqrt{d}}(\gamma + \dots + \epsilon) \quad (4.21)$$

and applying $\langle b_2| \dots |b_2\rangle$ to both sides gives

$$(\alpha + \beta + \dots + \epsilon) = \frac{1}{\sqrt{d}}(\gamma + \dots + \epsilon) \quad (4.22)$$

from which we conclude that $\beta = 0$ and we can similarly argue that $\gamma, \dots, \epsilon = 0$. Finally by applying $\langle a_1| \dots |a_1\rangle$ to both side of equation 4.20 we obtain $\alpha = 0$ hence the set in equation 4.15 are linearly independent.

We now show that for each of the Hermitian operators H given in equation 4.15 we can implement $U = \exp(i\theta H)$ for any $\theta \in \mathbb{R}$ by gates of the form $U(\vec{c})$.

We first note that if $c_j = 1$ for all j then $U(\vec{c})$ is the quantum Fourier transform F . We can also can construct any diagonal matrix $D(\vec{c}) = \text{diag}(c_0, \dots, c_{d-1})$ as follows

$$D(\vec{c}) = F^\dagger U(\vec{c}) = F^3 U(\vec{c}). \quad (4.23)$$

We can use this to construct the Clifford gate S

$$S = D(c_j = \omega^{\frac{j(j+1)}{2}}) \quad (4.24)$$

and also arbitrary rotations of the form

$$\exp(i\theta|j\rangle\langle j|) = D(c_0, \dots, \exp(i\theta\omega^j), \dots, c_{d-1}). \quad (4.25)$$

Then for any arbitrary element $P \in \mathcal{P}_d$ we have (as is shown in appendix A) $P = CZC^\dagger$ for some $C \in \mathcal{C}l_d$ and C is some product of F and S so C can be expressed in terms of $U(\vec{c})$. Then if $|\lambda\rangle$ is an eigenvector of P then for some $j \in \mathbb{Z}_d$ we have up to a phase $|\lambda\rangle = C|j\rangle$. It follows that

$$\exp(i\theta|\lambda\rangle\langle\lambda|) = \exp(i\theta C|j\rangle\langle j|C^\dagger) \quad (4.26)$$

$$= C \exp(i\theta|j\rangle\langle j|) C^\dagger. \quad (4.27)$$

□

Corollary 4.3. *Gates of the form $U(\vec{c})$ and C_Z are universal for d-level quantum computation*

Proof. In [26] it is shown that any entangling two-qudit gate together with all one-qudit gates provides exact universality on an arbitrary number of qudits. The authors show that the generalised controlled-Z gate C_Z is entangling and hence, by theorem 4.2, gates of the form $U(\vec{c})$ and C_Z are universal for d-level quantum computation. □

We remark that we can have an approximately universal gate set of $\{C_Z, F, D\}$ where we have chosen D to be a diagonal matrix where each entry is an irrational phase and each pair of phases differ by an irrational factor.

5 The d1WQC in the VBS formalism

We saw in section 3 that we can produce a cluster state by applying a projector of the form $\Pi = \sum_k |\tilde{k}\rangle\langle k| \dots \langle k|$ to all the VBS qudits at each cluster site to give the cluster qudits. In this section we show that the implementations of gate $U(\vec{c})$ and C_Z given in the last section are well aligned with this projector: upon projection, these gate implementations are naturally converted into a pattern of one-qudit measurements on the cluster state thus deriving the measurement schemes for this set of universal gates on the d1WQC.

5.1 Performing $U(\vec{c})$ in the d1WQC

Considering the two-qudit measurement basis we used in section 4.2.1 to implement the $U(\vec{c})$ gate

$$B = \{|\alpha_{st}\rangle = (U(\vec{c})^\dagger X^s Z^t \otimes I)|H\rangle : s, t \in \mathbb{Z}_d\}. \quad (5.1)$$

We observe that the post measurement states corresponding to the measurement result $t = 0$ all lie in the subspace of the projected cluster state since

$$(U(\vec{c})^\dagger X^s \otimes I)|H\rangle = (Z^s U(\vec{c})^\dagger \otimes I)C_Z|+\rangle|+\rangle \quad (5.2)$$

$$= (Z^{-s} \otimes I) \sum_{jkl} \bar{c}_l \omega^{j(k-l)} |l\rangle|k\rangle \quad (5.3)$$

$$= \sum_l \omega^{-sl} \bar{c}_l |l\rangle|l\rangle. \quad (5.4)$$

Since B is an orthogonal basis all the post measurement states corresponding to $t \neq 0$ lie in the orthogonal complement to this subspace. So from equation 4.3 we see that in the restriction to the cluster state obtained by the projector $\Pi = \sum_m |\tilde{m}\rangle\langle m|$ the final state of the second qudit is $X^{-s}U(\vec{c})$. From equation 5.4, the one-qudit basis B' as shown in figure 8 on the d1WQC is thus

$$B' = \left\{ \sum_l \omega^{-sl} \bar{c}_l |\tilde{l}\rangle \right\}_{s \in \mathbb{Z}_d} = \left\{ U^\dagger(\vec{c})|\tilde{s}\rangle \right\}_{s \in \mathbb{Z}_d} \quad (5.5)$$

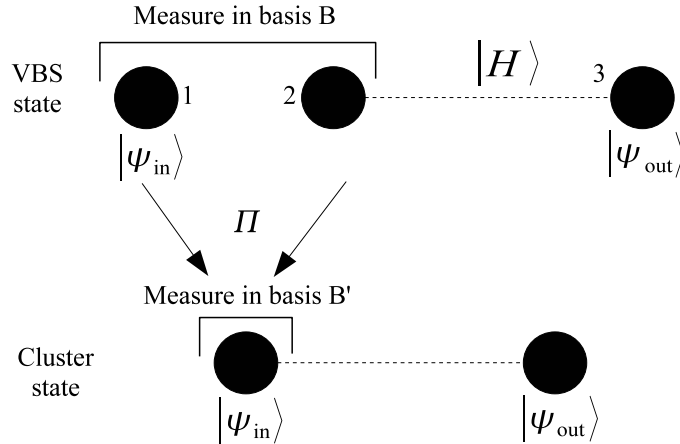


Figure 8: Implementing $U(\vec{c})$ on the d1WQC

Hence the effect of Π is to restrict the outcomes of the B measurement to have $t = 0$, which is equivalent to performing a one-qudit measurement in basis B' on the cluster state qudit.

By combining these measurements along a one dimensional cluster state and adaptively altering the basis to propagate Pauli errors to the end of the computation we can implement any one-qudit operation on the d1WQC. Next we will see how to implement the two-qudit gate controlled-Z.

5.2 Performing C_Z in the d1WQC

If we project the VBS state in figure 7, which is used to implement the C_Z gate, down to a cluster state we will obtain the state shown in figure 9. Furthermore it is clear that the elements of the basis B_2 defined in equation 4.9 for which $r, t = 0$ lie in the projected cluster state and the elements $r, t \neq 0$ lie in its orthogonal complement. We consider the action of both measurements in the basis B_2 with corresponding measurement results r, s, t and u, v, w . When restricted to $r, t, u, w = 0$, which corresponds to the action on the projected cluster state shown in figure 7, this produces, by lemma 4.1, the output

$$|\psi_{out}^1\rangle_1 |\psi_{out}^2\rangle_2 = X_1^s X_2^v F_1 F_2 C_{Z(1,2)} |\psi_{in}^1\rangle_1 |\psi_{in}^2\rangle_2. \quad (5.6)$$

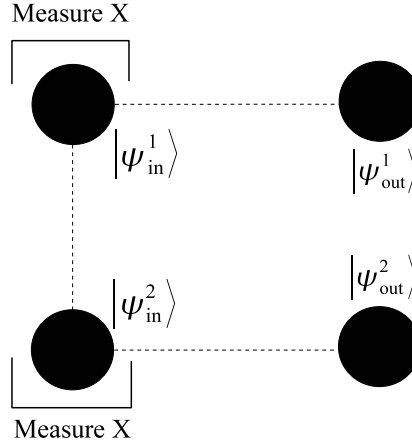


Figure 9: Implementing a generalised C_Z gate on the d1WQC

Thus the measurement scheme to implement C_Z on the d1WQC is obtained by applying the usual projector, Π , to the basis B_2 . Let $|b\rangle$ be an arbitrary basis vector corresponding to the measurement result $r, t = 0$ such that $|b\rangle = (I \otimes Z^s \otimes I) \sum_m |m\rangle |m\rangle |m\rangle$ then

$$\Pi|b\rangle = \sum_k |\tilde{k}\rangle \langle k| \langle k| \langle k| (I \otimes Z^s \otimes I) \sum_m |m\rangle |m\rangle |m\rangle \quad (5.7)$$

$$= \sum_{km} \omega^{sm} |\tilde{k}\rangle \langle k| \langle k| \langle k| |m\rangle |m\rangle |m\rangle \quad (5.8)$$

$$= \sum_k \omega^{sk} |\tilde{k}\rangle. \quad (5.9)$$

The scheme to implement C_Z on the d1WQC, as shown in figure 7, is to measure the two input qudits in the basis $\{F|s\rangle\}_{s \in Z_d}$ which is a measurement in the X basis. We must then implement the inverse Fourier transform F^\dagger on both qudits and by equation 5.6 we will have implemented C_Z up to a known Pauli error.

6 Parallel complexity of d1WQC and extensions of the model

We see from the construction of the d1WQC, in section 4.2.2 that the only adaptations of measurements that we have to make are when we propagate the teleportation errors from the Pauli group through the gates of the form $U(\vec{c})$. In the case where we wish to implement one-qudit Clifford gates, we may leave our implementation involving $U(\vec{c})$ gate unchanged and calculate the propagation of the Pauli errors through the Clifford gate. In this way if the circuit we wish to implement is a Clifford circuit then we may apply all the one-qudit measurements on the d1WQC in parallel.

The VBS formalism that we have described provides a fundamental connection between d1WQC and the process of teleportation and this relationship leads to a wide class of natural extensions and generalisations of 1WQC. Werner [24] has shown that there exists a wide variety of inequivalent teleportation schemes in dimensions greater than 2. For example any set of operators that form a unitary operator basis may be used to construct a teleportation scheme. Furthermore it can be shown that even in dimension 2 there exist still more possible teleportation schemes in which the Bell measurement is replaced by a POVM [27].

Any of these teleportation schemes may then be used in a VBS setting resulting in new classes of measurement-based models of quantum computation. In each such formalism we have a set of “teleportation correction operators” analogous to the Pauli operations in standard teleportation, and an associated normaliser group. Circuits of the latter operators would then lead to further new classes of parallelisable quantum algorithms. These issues will be developed in a later paper.

7 Conclusion

We have shown how to interpret the workings of d-level one-way quantum computation in terms of d-level valence bond solids. We constructed cluster states of qudits using this formalism and derived implementations of a universal set of gates on the d1WQC using one-qudit measurements. We also showed that, analogously to the qubit case, the set of circuits in the Clifford group, $\mathcal{Cl}_d^{\otimes n}$, can be implemented in one parallel time step of quantum measurements on the d1WQC followed by some classical computation and we have characterised the structure of the Clifford group for spaces of prime dimension.

Acknowledgements

I would like to thank Richard Jozsa for much advice and help during the production of this paper and Ashley Montanaro, Noah Linden, Andreas Winter, Tobias Osborne and David Fattal for helpful discussions. This work was supported by the UK Engineering and Physical Sciences Research Council QIP-IRC grant and the U.K. Government Communications Head Quarters.

Note added in proof: after this paper was completed we noticed the appearance of [28] which treats some of the same issues from a different perspective.

Appendix A: Generating the Clifford group for d-level systems where d is prime

In this appendix we fully characterise the Clifford group $\mathcal{Cl}_d^{\otimes n}$, for the case where d is an odd prime, by showing that all its elements can be generated, up to a global phase factor, by circuits consisting of C_X , F and S as defined in section 2.

We note the following commutation properties

$$ZX = \omega XZ \text{ and } (Z^a X^b)(Z^c X^d) = \omega^{ad-bc}(Z^c X^d)(Z^a X^b). \quad (\text{A.1})$$

If we write $P = (Z_1^{a_1} X_1^{b_1} \dots Z_n^{a_n} X_n^{b_n})$ and $Q = (Z_1^{c_1} X_1^{d_1} \dots Z_n^{c_n} X_n^{d_n})$ then

$$PQ = \omega^{\sum_{i=1}^n a_i d_i - b_i c_i} QP = \omega^{(P,Q)} QP \quad (\text{A.2})$$

where we use the following notation

$$(P, Q) = \sum_{i=1}^n a_i d_i - b_i c_i. \quad (\text{A.3})$$

The generalised Clifford group $\mathcal{Cl}_d^{\otimes n}$ on n qudits is defined in definition 2.2 as the normaliser of $\mathcal{P}_d^{\otimes n}$. Each $C \in \mathcal{Cl}_d^{\otimes n}$ induces an endomorphism of $\mathcal{P}_d^{\otimes n}$ by its action under conjugation. We write

$$P \mapsto_C Q \text{ for } P, Q \in \mathcal{P}_d^{\otimes n} \text{ when } CPC^{-1} = Q. \quad (\text{A.4})$$

Sometimes it will be useful to consider two elements $P, Q \in \mathcal{P}_d^{\otimes n}$ as equivalent if they differ only by a global phase. In this way we can represent each member $cZ_1^{a_1} X_1^{b_1} \dots Z_n^{a_n} X_n^{b_n} \in \mathcal{P}_d^{\otimes n}$ (where c is a phase) up to global phase as:

$$(a_1, b_1, \dots, a_n, b_n) \in \mathbb{Z}_d^{2n}. \quad (\text{A.5})$$

In view of the commutation relation A.2, products in $\mathcal{P}_d^{\otimes n}$ correspond up to a phase to addition of the corresponding vectors in \mathbb{Z}_d^{2n} . Furthermore the action of Clifford operations is linear: if we use elements in $\{Z_1, X_1, \dots, Z_n, X_n\}$, where Z_i is the n -qudit operator which acts as Z on qubit i and the identity elsewhere, as a basis of $\mathcal{P}_d^{\otimes n}$ we can represent the action of C up to a global phase as a $2n \times 2n$ matrix $M(C)$ with entries in \mathbb{Z}_d .

F and S induce the following mappings on \mathcal{P}_d

$$X \mapsto_F Z \text{ and } Z \mapsto_F X^{-1} \quad (\text{A.6})$$

$$Z \mapsto_S Z \text{ and } X \mapsto_S ZX \quad (\text{A.7})$$

so the matrix representations $M(F)$ and $M(S)$ are

$$M(F) \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ -a \end{pmatrix} \quad (\text{A.8})$$

$$M(S) \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a+b \\ b \end{pmatrix}. \quad (\text{A.9})$$

Lemma 7.1. F^{-1} , S^{-1} , Z , X , Z^{-1} and X^{-1} can all be constructed from $\{F, S\}$.

Proof. Firstly we note that $F^4 = I$ so $F^{-1} = F^3$ and $S^d = I$ so $S^{-1} = S^{d-1}$. Then we have

$$Z = F^2 S^{-1} F^2 S. \quad (\text{A.10})$$

Then since $Z^d = I$ we have $Z^{-1} = Z^{d-1}$. We can use this to construct X since

$$X = F Z^{-1} F^{-1}. \quad (\text{A.11})$$

Finally we have $X^d = I$ so $X^{-1} = X^{d-1}$. \square

$C_X \in \mathcal{Cl}_d^{\otimes 2}$ can be seen from the following mappings on $\mathcal{P}_d^{\otimes 2}$

$$Z_1 \mapsto_{C_X} Z_1, X_1 \mapsto_{C_X} X_1 X_2, Z_2 \mapsto_{C_X} Z_1^{-1} Z_2, X_2 \mapsto_{C_X} X_2. \quad (\text{A.12})$$

Similarly $C_Z \in \mathcal{Cl}_d^{\otimes 2}$ since

$$Z_1 \mapsto_{C_Z} Z_1, X_1 \mapsto_{C_Z} X_1 Z_2, Z_2 \mapsto_{C_Z} Z_2, X_2 \mapsto_{C_Z} Z_1 X_2. \quad (\text{A.13})$$

Since the normalising property of actions is preserved by composition and tensor product we see that any gate that can be constructed (in the quantum circuit sense [29]) from gates in the Clifford group must itself be in the Clifford group.

Lemma 7.2. C_Z can be constructed from $\{C_X, F\}$

Proof.

$$C_{Z(1,2)} = F_2 C_{X(1,2)} F_2^{-1}. \quad (\text{A.14})$$

\square

Definition 7.3. An arbitrary controlled Pauli operator $C_{X^s Z^t}$ with $s, t \in \mathbb{Z}_d$ is defined as

$$C_{X^s Z^t} |j\rangle |k\rangle = |j\rangle (X^s Z^t)^j |k\rangle \quad (\text{A.15})$$

$$= \omega^{\frac{stj(j-1)}{2} + tjk} |j\rangle |k + sj\rangle. \quad (\text{A.16})$$

This then produces the following mappings

$$Z_1 \mapsto_{C_{X^s Z^t}} Z_1, X_1 \mapsto_{C_{X^s Z^t}} X_1 X_2^s Z_2^t, Z_2 \mapsto_{C_{X^s Z^t}} Z_1^{-s} Z_2, X_2 \mapsto_{C_{X^s Z^t}} Z_1^t X_2. \quad (\text{A.17})$$

Lemma 7.4. $C_{X^s Z^t}$ can be constructed from $\{C_X, F, S\}$ if the qudit dimension d is an odd integer.

Remark: If d is an even integer then the definition of S needs to be modified in order for it to be a valid Clifford operation, and then this lemma remains valid.

Proof. We have already seen in equation A.15 that

$$C_{X^s Z^t} |j\rangle |k\rangle = \omega^{\frac{stj(j-1)}{2}} (C_X)^s (C_Z)^t |j\rangle |k\rangle \quad (\text{A.18})$$

where C_Z is suitably constructed (by lemma 7.2). We note that since d is an odd integer

$$S |j\rangle = \omega^{\frac{j(j+1)}{2}} |j\rangle \quad (\text{A.19})$$

$$SZ^{-1} |j\rangle = \omega^{\frac{j(j-1)}{2}} |j\rangle \quad (\text{A.20})$$

$$C_{X^s Z^t} = (C_X)^s (C_Z)^t (SZ^{-1})_1^{st}. \quad (\text{A.21})$$

□

Definition 7.5. The *SWAP* gate is defined as $SWAP |j\rangle |k\rangle = |k\rangle |j\rangle$.

Lemma 7.6. *SWAP* can be constructed from $\{C_X, F\}$.

Proof. We can construct a C_X gate that uses the second qudit as control and the first as target

$$C_{X(2,1)} = F_1 F_2^{-1} C_{X(1,2)} F_1^{-1} F_2. \quad (\text{A.22})$$

Then *SWAP* is constructed using the following identity

$$SWAP = C_{X(1,2)} C_{X(2,1)}^{-1} C_{X(1,2)} F_2^2 \quad (\text{A.23})$$

where, since $C_{X(2,1)}^d = I \otimes I$ we have $C_{X(2,1)}^{-1} = C_{X(2,1)}^{d-1}$. □

The construction of the *SWAP* gate from the gate set $\{C_X, F, S\}$ allows constructions in which multiple qudit gates can be applied to non-local qudits. Often the quantum circuit model allows for non-local applications of two-qudit gates. The above lemma shows that such an assumption is not necessary for the construction of the Clifford group.

Now we turn our attention to associations defined on subsets of the the Pauli group.

Definition 7.7. Let $\{P_i\}$ and $\{\bar{P}_i\}$ be any subsets of $\mathcal{P}_d^{\otimes n}$ of the same size. We say that the association $P_i \mapsto \bar{P}_i$ is commutation relation preserving (CRP) if

$$(P_i, P_j) = (\bar{P}_i, \bar{P}_j) \text{ for all } i, j. \quad (\text{A.24})$$

Lemma 7.8. *The maps induced by conjugation with Clifford group operations are CRP on $\mathcal{P}_d^{\otimes n}$.*

Proof. For any $P, Q \in \mathcal{P}_d^{\otimes n}$ we have $PQ = \omega^{(P,Q)} QP$ so for $U \in Cl_d^{\otimes n}$ we have

$$(UPU^{-1})(UQU^{-1}) = U(PQ)U^{-1} = \omega^{(P,Q)} U(QP)U^{-1} = \omega^{(P,Q)} (UQU^{-1})(UPU^{-1}). \quad (\text{A.25})$$

□

Lemma 7.9. *Given any CRP association A of one-qudit Pauli operators $Z \mapsto Z^a X^b$ and $X \mapsto Z^c X^d$ we can construct an operator from $\{F, S\}$ whose action generates this association.*

Proof. In terms of the representation of equation A.5, the matrix of the association A is

$$M(A) = \begin{pmatrix} a & c \\ b & d \end{pmatrix}. \quad (\text{A.26})$$

From equation A.1 and the fact that A is CRP we can deduce that

$$ad - bc = 1 \quad (\text{A.27})$$

so $M(A) \in SL(2, \mathbb{Z}_d)$. In [30] it is shown that the matrices $M(S)$ and $M(F)$ in equations A.8 and A.9 generate $SL(2, \mathbb{Z}_d)$. Hence any such $M(A)$ can be generated by $M(F)$ and $M(S)$. \square

Having established this result for CRP associations defined on \mathcal{P}_d we now extend this to $\mathcal{P}_d^{\otimes n}$. An outline of the remainder of the proof is as follows: In lemma 7.10 we show that given $P, Q \in \mathcal{P}_d^{\otimes n}$ such that $P = Z_1^{a_1} X_1^{b_1} \dots Z_n^{a_n} X_n^{b_n}$ and $Q = Z_1^{c_1} X_1^{d_1} \dots Z_n^{c_n} X_n^{d_n}$ we may assume wlog (modulo some suitable mapping constructed from $\{C_X, F, S\}$) that there exists some $j \in \{1, \dots, n\}$ such that $a_j d_j - b_j c_j = 1$. In lemma 7.11 we show that if $(P, Q) = 1$ then we can assume wlog (modulo some mapping constructed from $\{C_X, F, S\}$) that $P = X \otimes P'$ and $Q = Z \otimes Q'$. Then we take some arbitrary CRP association $X_i \mapsto \bar{X}_i$ and $Z_i \mapsto \bar{Z}_i$ and the main part of the proof is to establish that it may be constructed from $\{C_X, F, S\}$. In lemma 7.12 we take such a CRP association and assume that $\bar{X}_1 = X \otimes P'$ and $\bar{Z}_1 = Z \otimes Q'$ and construct a gate U from $\{C_X, F, S\}$ such that $X_1 \mapsto_U X \otimes P'$ and $Z_1 \mapsto_U Z \otimes Q'$. Taking this gate U we show in lemma 7.13 that there exists $R_i, S_i \in \mathcal{P}_d^{\otimes n-1}$ such that $I \otimes R_i \mapsto_U \bar{X}_i$ and $I \otimes S_i \mapsto_U \bar{Z}_i$. Using the Pauli elements R_i and S_i we show in lemma 7.14 that the $n-1$ qudit association V defined by $X_i \mapsto_V I \otimes R_i$ and $Z_i \mapsto_V I \otimes S_i$ is CRP. This leads to lemma 7.15 in which we show that the arbitrary association $X_i \mapsto \bar{X}_i$ and $Z_i \mapsto \bar{Z}_i$ is satisfied by the mapping induced by $U(I \otimes V)$. Using the preceding results we proceed by induction in theorem 7.16 to show that any such CRP association can be constructed from $\{C_X, F, S\}$ and in corollary 7.17 that $\mathcal{Cl}_d^{\otimes n}$ is generated by $\{C_X, F, S\}$ when d is prime.

Lemma 7.10. *Given $P, Q \in \mathcal{P}_d^{\otimes n}$ such that $(P, Q) = 1$ and*

$$P = Z_1^{a_1} X_1^{b_1} \dots Z_n^{a_n} X_n^{b_n}, \quad Q = Z_1^{c_1} X_1^{d_1} \dots Z_n^{c_n} X_n^{d_n} \quad (\text{A.28})$$

there exists a construction M from $\{C_X, F, S\}$ such that

$$P \mapsto_M Z_1^{a'_1} X_1^{b'_1} \dots Z_n^{a'_n} X_n^{b'_n} \quad \text{and} \quad Q \mapsto_M Z_1^{c'_1} X_1^{d'_1} \dots Z_n^{c'_n} X_n^{d'_n} \quad (\text{A.29})$$

and there exists $j \in \{1, \dots, n\}$ with $a'_j d'_j - b'_j c'_j = 1$.

Proof. Since $(P, Q) = 1$ we have

$$\sum_{i=1}^n a_i d_i - b_i c_i = 1 \quad (\text{A.30})$$

so we can choose j such that

$$a_j d_j - b_j c_j \neq 0. \quad (\text{A.31})$$

If $a_j d_j - b_j c_j = 1$ then the mapping M is trivial and the proof completes. Otherwise there must exist $k \neq j$ such that

$$a_k d_k - b_k c_k \neq 0. \quad (\text{A.32})$$

The construction for M follows. Firstly if $b_j \neq 0$ we take g such that $a_j + g b_j = 0$ (the existence of such a g following from d being prime) and apply FS^g to P and Q by conjugation to the j^{th} qudit. This maps P to \bar{P} , say, where \bar{P} is of the form such that $\bar{b}_j = 0$. Given this mapping let us assume that the original P was of the form such that

$$b_j = 0. \quad (\text{A.33})$$

We apply by conjugation a $C_{X^s Z^t}$ gate to P and Q with the j^{th} qudit as control and k^{th} qudit as target. Using the relations given in equation A.17 we obtain

$$a'_j = a_j - s a_k + t b_k, \quad b'_j = b_j \quad (\text{A.34})$$

$$c'_j = c_j - s c_k + t d_k, \quad d'_j = d_j. \quad (\text{A.35})$$

Hence given $b_j = 0$ we have

$$a'_j d'_j - b'_j c'_j = (a_j - s a_k + t b_k) d_j. \quad (\text{A.36})$$

We observe from equation A.32 that a_k and b_k can not both be zero and since $d_j \neq 0$ (by equations A.31 and A.33) we can choose $s, t \in \mathbb{Z}_d$ such that

$$(a_j - s a_k + t b_k) d_j = 1 \quad (\text{A.37})$$

by the fact that d is prime. Hence we have $a'_j d'_j - b'_j c'_j = 1$ as desired. \square

Lemma 7.11. *Given $P, Q \in \mathcal{P}_d^{\otimes n}$ such that $(P, Q) = 1$ there is a construction W from $\{C_X, F, S\}$ such that $P \mapsto_W X \otimes P'$ and $Q \mapsto_W Z \otimes Q'$ for some $P', Q' \in \mathcal{P}_d^{\otimes n-1}$.*

Proof. Using the same notation as, and by an application of, lemma 7.10 we assume wlog that for some $j \in \{1, \dots, n\}$

$$a_j d_j - b_j c_j = 1. \quad (\text{A.38})$$

We construct W by performing a *SWAP* between the 1^{st} and j^{th} qudits followed by a one-qudit mapping induced by L on the 1^{st} qudit where the matrix of L is

$$M(L) = \begin{pmatrix} d_j & -c_j \\ -b_j & a_j \end{pmatrix}. \quad (\text{A.39})$$

L produces the desired mapping since

$$Z^{a_j} X^{b_j} \mapsto_L X, Z^{c_j} X^{d_j} \mapsto_L Z. \quad (\text{A.40})$$

Furthermore since $M(L)$ has unit determinant it can be constructed from $\{F, S\}$ by lemma 7.9. \square

Lemma 7.12. *Suppose we have a CRP association $X_i \mapsto \bar{X}_i$ and $Z_i \mapsto \bar{Z}_i$ defined on $\mathcal{P}_d^{\otimes n}$ where d is an odd prime and let us assume wlog (by lemma 7.11) that $\bar{X}_1 = X \otimes P'$ and $\bar{Z}_1 = Z \otimes Q'$ with $P', Q' \in \mathcal{P}_d^{\otimes n-1}$. Then there exists a construction U from $\{C_X, F, S\}$ such that $X_1 \mapsto_U X \otimes P'$ and $Z_1 \mapsto_U Z \otimes Q'$.*

Proof. Let us write

$$X \otimes P' = Z_1^{a_1} X_1^{b_1} \dots Z_n^{a_n} X_n^{b_n} \quad (\text{A.41})$$

$$Z \otimes Q' = Z_1^{c_1} X_1^{d_1} \dots Z_n^{c_n} X_n^{d_n} \quad (\text{A.42})$$

We construct a circuit P'_{impl} from P' in which we perform $C_{X^{b_i} Z^{a_i}}$ between the 1^{st} and the i^{th} qudit (using the 1^{st} as control) for each $i \in \{2, \dots, n\}$. We repeat the construction of P'_{impl} with the indices of Q' to produce Q'_{impl} . The construction of U is then

$$U = F_1 Q'_{impl} F_1^{-1} P'_{impl}. \quad (\text{A.43})$$

We now justify this construction. The image of Z_1 by U can be seen to be $Z \otimes Q'$ from the following sequence of mappings:

$$Z_1 \mapsto_{P'_{impl}} Z_1 \mapsto_{F_1^{-1}} X_1 \mapsto_{Q'_{impl}} X \otimes Q' \mapsto_{F_1} Z \otimes Q' \quad (\text{A.44})$$

where we have used the mappings in A.17 to deduce that Z_1 commutes with each $C_{X^{b_i} Z^{a_i}(1,i)}$ from P'_{impl} and the image of X_1 under conjugation with each $C_{X^{d_i} Z^{c_i}(1,i)}$ from Q'_{impl} is $X_1 Z_i^{c_i} X_i^{d_i}$.

Now let us look at the image of X_1 when conjugated by U we have

$$X_1 \mapsto_{P'_{impl}} X \otimes P' \mapsto_{F_1^{-1}} Z_1^{-1} \otimes P'. \quad (\text{A.45})$$

Then Z_1^{-1} commutes with Q'_{impl} and is mapped to X_1 by the final F_1 . We must consider the image of the elements of P' by Q'_{impl} . The image of $Z_i^{a_i} X_i^{b_i}$ on the target qudit under the action of $C_{X_i^{d_i} Z_i^{c_i}}$ is $Z^{b_i c_i - a_i d_i}$ on the control and $Z^{a_i} X^{b_i}$ on the target and the target is as desired. The contribution to the power of Z on the control by the image of P' by Q'_{impl} is then

$$\sum_{i=2}^n b_i c_i - a_i d_i. \quad (\text{A.46})$$

Since the mapping is CRP we have

$$1 = (X_1, Z_1) = (X \otimes P', Z \otimes Q') = \sum_{i=1}^n a_i d_i - b_i c_i. \quad (\text{A.47})$$

Furthermore $a_1 d_1 - b_1 c_1 = 1$ so $\sum_{i=2}^n b_i c_i - a_i d_i = 0$ and hence $X_1 \mapsto_U X \otimes P'$ as desired. \square

Lemma 7.13. *The Clifford circuit U in lemma 7.12 has the property that*

$$I \otimes R_i \mapsto_U \bar{X}_i \text{ and } I \otimes S_i \mapsto_U \bar{Z}_i \quad (\text{A.48})$$

for some $R_i, S_i \in \mathcal{P}_d^{\otimes n-1}$ and all $i \in \{2, \dots, n\}$.

Proof. Since U is a Clifford operation so is U^{-1} . We have the CRP map $X_i \mapsto \bar{X}_i \mapsto_{U^{-1}} \bar{X}'_i$ and $Z_i \mapsto \bar{Z}_i \mapsto_{U^{-1}} \bar{Z}'_i$. For $i \in \{2, \dots, n\}$ \bar{X}'_i commutes with both X_1 and Z_1 and so is of the form $I \otimes R_i$. Similarly \bar{Z}'_i commutes with both X_1 and Z_1 and is of the form $I \otimes S_i$. \square

Lemma 7.14. *The $n-1$ qudit association V (acting on qudits 2 to n) given by $X_i \mapsto_V I \otimes R_i$ and $Z_i \mapsto_V I \otimes S_i$ for $i \in \{2, \dots, n\}$ is CRP.*

Proof. Since $X_i \mapsto \bar{X}_i \mapsto_{U^{-1}} I \otimes R_i$ and $Z_i \mapsto \bar{Z}_i \mapsto_{U^{-1}} I \otimes S_i$ is CRP we have for $i, j \in \{2, \dots, n\}$

$$(S_i, S_j) = (X_i, X_j) = 0, (R_i, R_j) = (Z_i, Z_j) = 0, (S_i, R_j) = (X_i, X_j) = \delta_{ij}. \quad (\text{A.49})$$

Hence V is CRP. \square

Lemma 7.15. *The mapping induced by $U(I \otimes V)$ where U and V are defined in lemmas 7.12 and 7.14 is such that*

$$X_i \mapsto_{U(I \otimes V)} \bar{X}_i \text{ and } Z_i \mapsto_{U(I \otimes V)} \bar{Z}_i \quad (\text{A.50})$$

Proof. The result follows from:

$$X_1 \mapsto_{I \otimes V} X_1 \mapsto_U X \otimes P' = \bar{X}_1, Z_1 \mapsto_{I \otimes V} Z_1 \mapsto_U Z \otimes Q' = \bar{Z}_1 \quad (\text{A.51})$$

and

$$X_i \mapsto_{I \otimes V} I \otimes R_i \mapsto_U \bar{X}_i, Z_i \mapsto_{I \otimes V} I \otimes S_i \mapsto_U \bar{Z}_i \text{ for } i \in \{2, \dots, n\}. \quad (\text{A.52})$$

\square

Theorem 7.16. *Any CRP association $X_i \mapsto \bar{X}_i$ and $Z_i \mapsto \bar{Z}_i$ for $i \in \{1, \dots, n\}$ defined on $\mathcal{P}_d^{\otimes n}$ where d is an odd prime can be constructed from $\{C_X, F, S\}$.*

Proof. We proceed by induction on n where the base of $n = 1$ is provided by lemma 7.9. We assume that any CRP association on $(n-1)$ qudits can be constructed from $\{C_X, F, S\}$. For the n -qudit CRP association $X_i \mapsto \bar{X}_i, Z_i \mapsto \bar{Z}_i$ there exists, by lemma 7.11, a construction W from $\{C_X, F, S\}$ such that $\bar{X}_1 \mapsto_W X \otimes P'$ and $\bar{Z}_1 \mapsto_W Z \otimes Q'$. Suppose W maps $\bar{X}_i \mapsto \bar{X}'_i$ and $\bar{Z}_i \mapsto \bar{Z}'_i$. By lemmas 7.12, 7.14 and 7.15 there exists a CRP map $U(I \otimes V)$ which maps $X_i \mapsto \bar{X}'_i$ and $Z_i \mapsto \bar{Z}'_i$. So $W^{-1}U(I \otimes V)$ maps $X_i \mapsto \bar{X}_i$ and $Z_i \mapsto \bar{Z}_i$. U has a construction from $\{C_X, F, S\}$ by 7.12 and since V acts on $n-1$ qudits there exists a construction for it from $\{C_X, F, S\}$ by the inductive hypothesis. \square

Corollary 7.17. *The Clifford group on n qudits is generated by $\{C_X, F, S\}$ when the dimension d of a qudit is an odd prime.*

Proof. Any Clifford group mapping is fully defined by its action on X_i and Z_i . Furthermore, by lemma 7.8 this association is CRP, so by theorem 7.16 it can be constructed from $\{C_X, F, S\}$. \square

Appendix B: Proof of lemma 4.1

Proof. The state of the system in figure 7 before measurement is

$$\begin{aligned}
|VBS\rangle &= |\psi_{in}^1\rangle_1 |\psi_{in}^2\rangle_5 |H\rangle_{26} |H\rangle_{34} |H\rangle_{78} \\
&= \left(\sum_a \psi_a^1 |a\rangle_1 \right) \left(\sum_b \psi_b^2 |b\rangle_5 \right) \left(\sum_{c,d} \omega^{cd} |c\rangle_2 |d\rangle_6 \right) \left(\sum_{e,f} \omega^{ef} |e\rangle_3 |f\rangle_4 \right) \left(\sum_{g,h} \omega^{gh} |g\rangle_7 |h\rangle_8 \right) \\
&= \sum_{abcdefgh} \psi_a^1 \psi_b^2 \omega^{cd+ef+gh} |a\rangle_1 |c\rangle_2 |e\rangle_3 |f\rangle_4 |b\rangle_5 |d\rangle_6 |g\rangle_7 |h\rangle_8
\end{aligned}$$

If the measurement results are $r, s, t, u, v, w \in \mathbb{Z}_d$ then the following projector is applied to the VBS state

$$\sum_{mnpq} \omega^{s(m-n)+v(p-q)} |m+r\rangle_1 |m\rangle_2 |m+t\rangle_3 |p+u\rangle_5 |p\rangle_6 |p+w\rangle_7 \langle n+s|_1 \langle n|_2 \langle n+t|_3 \langle q+u|_5 \langle q|_6 \langle q+w|_7 \quad (\text{B.1})$$

Applying Π_{B_2} to $|VBS\rangle$ we get six indices removed with the following relations

$$a = n + r, b = q + u, c = n, d = q, e = n + t, g = q + w \quad (\text{B.2})$$

giving

$$\Pi_{B_2} |VBS\rangle = \sum_{mnpqfh} \psi_{n+r}^1 \psi_{q+u}^2 \omega^{s(m-n)+v(p-q)+nq+nf+tf+qh+wh} \quad (\text{B.3})$$

$$|m+r\rangle_1 |m\rangle_2 |m+t\rangle_3 |f\rangle_4 |p+u\rangle_5 |p\rangle_6 |p+w\rangle_7 |h\rangle_8 \quad (\text{B.4})$$

$$= \left(\sum_{nqfh} \psi_{n+r}^1 \psi_{q+u}^2 \omega^{-sn-vq+nq+nf+tf+qh+wh} |f\rangle_4 |h\rangle_8 \right) \quad (\text{B.5})$$

$$\otimes (\dots)_{123567} \quad (\text{B.6})$$

The restriction to qudits 4 and 8 of this state is recognised with a simple calculation as

$$Z_4^t Z_8^w F_4 F_8 C_{Z(4,8)} Z_4^{-s} Z_8^{-v} X_4^{-r} X_8^{-u} |\psi_{in}^1\rangle_4 |\psi_{in}^2\rangle_8. \quad (\text{B.7})$$

We can propagate all the Pauli terms to the left hand side of the expression using the propagation relations given in equations A.6 and A.13 so that equating up to a global phase

$$Z_4^t Z_8^w F_4 F_8 C_{Z(4,8)} Z_4^{-s} Z_8^{-v} X_4^{-r} X_8^{-u} = Z_4^{t-r} Z_8^{w-u} X_4^{s+u} X_8^{v+r} F_4 F_8 C_{Z(4,8)} \quad (\text{B.8})$$

\square

References

- [1] Robert Raussendorf and Hans J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86:5188–5191, 2001.
- [2] Robert Raussendorf, Daniel E. Browne, and Hans J. Briegel. Measurement-based quantum computation on cluster states. *Phys. Rev. A*, 68:022312, 2003. quant-ph/0301052.
- [3] Robert Raussendorf and Hans J. Briegel. Computational model underlying the one-way quantum computer. *quant-ph/0108067*, August 2001.
- [4] Michael A. Nielsen. Optical quantum computation using cluster states. *Phys. Rev. Lett.*, 93:040503, 2004. quant-ph/0402005.
- [5] Michael A. Nielsen and Christopher M. Dawson. Fault-tolerant quantum computation with cluster states. *Phys. Rev. A*, 71:042323, 2004. quant-ph/0405134.
- [6] Daniel E. Browne and Terry Rudolph. Resource efficient linear optical quantum computation. *Phys. Rev. Lett.*, 95:010501, 2004.
- [7] Yaakov S. Weinstein, C. Stephen Hellberg, and Jeremy Levy. Quantum dot cluster state computing with encoded qubits. *quant-ph/0506032*, June 2005.
- [8] P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger. Experimental one-way quantum computing. *Nature*, 434:169–176, 2005.
- [9] Panos Aliferis and Debbie W. Leung. Computation by measurements: a unifying picture. *Phys. Rev. A*, 70:062314, 2004. quant-ph/0404082.
- [10] Philippe Jorrand and Simon Perdrix. Unifying quantum computation with projective measurements only and one-way quantum computation. *quant-ph/0404125*, April 2004.
- [11] Andrew M. Childs, Debbie W. Leung, and Michael A. Nielsen. Unified derivations of measurement-based schemes for quantum computation. *Phys. Rev. A*, 71:032318, 2004. quant-ph/0404132.
- [12] F. Verstraete and J.I. Cirac. Valence bond solids for quantum computation. *Phys. Rev. A*, 70:060302, 2003.
- [13] Richard Jozsa. An introduction to measurement based quantum computation. *quant-ph/0508124*, August 2005.
- [14] Michael A. Nielsen. Universal quantum computation using only projective measurement, quantum memory, and the preparation of the $|0\rangle$ state. *quant-ph/0108020*, August 2001.
- [15] D. W. Leung. Two-qubit projective measurements are universal for quantum computation. *quant-ph/0111122*, November 2001.

- [16] D.L. Zhou, B. Zeng, Z. Xu, and C.P. Sun. Quantum computation based on d-level cluster state. *Phys. Rev. A*, 68(6):062303, 2003. quant-ph/0304054.
- [17] Mo-Lin Ge, Xu-Feng Liu, and Chang-Pu Sun. The cyclic representations of the quantum algebra $u_q(osp(2, 1))$ in terms of the z^n -algebra. *J. Phys. A: Math. Gen.*, 25:2907–2909, 1992.
- [18] Eric Hostens, Jeroen Dohaene, and Bert de Moor. Stabilizer states and clifford operations for systems of arbitrary dimensions, and modular arithmetic. *Phys. Rev. A*, 71:042315, 2004. quant-ph/0408190.
- [19] Daniel Gottesman. Stabilizer codes and quantum error correction. *quant-ph/9705052*, May 1997. PhD thesis.
- [20] Hans J. Briegel and Robert Raussendorf. Persistent entanglement in arrays of interacting particles. *Phys. Rev. Lett.*, 86(5):910–913, 2001.
- [21] Heng Fan, Vladimir Korepin, and Vwani Roychowdhury. Entanglement in a valence-bond-solid state. *Phys. Rev. Lett.*, 93:227203, 2004. quant-ph/0406067.
- [22] Heng Fan, Vladimir Korepin, and Vwani Roychowdhury. Valence-bond-solid state entanglement in a 2-d cayley tree. *quant-ph/0511150*, November 2005.
- [23] Charles H. Bennett, Giles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70(13):1895–1899, 1993.
- [24] R. F. Werner. All teleportation and dense coding schemes. *J. Phys. A: Math. Gen.*, 34:7081–7094, 2001. quant-ph/0003070.
- [25] Authur O. Pittenger and Mornton H. Rubin. Mutually unbiased bases, generalized spin matrices and separability. *quant-ph/0308142*, April 2003.
- [26] J. Brylinski and R. Brylinski. Universal quantum gates. *quant-ph/0108062*, August 2001.
- [27] Asher Peres. *Quantum Theory: Concepts and Methods*. Kluwer Academic Publishers, 1st edition, 1993.
- [28] William Hall. Cluster state quantum computation for many-level systems. *quant-ph/0512130*, December 2005.
- [29] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, New York, NY, USA, 2000.
- [30] Serge Lang. *Algebra*. Addison-Wesley, 3rd revised edition, 1993. pages 69-70.